地方独立行政法人大阪市立工業研究所情報セキュリティ運用規程

制定　平成２７年３月２５日　　規程第６７５号

第１章　総則

（目的）

第１条　この規程は、地方独立行政法人大阪市立工業研究所情報セキュリティ基本方針（以下「基本方針」という。）に基づき、地方独立行政法人大阪市立工業研究所（以下「法人」という。）が情報セキュリティを確保するために必要な事項を定めることを目的とする。

（定義）

第２条　この規程において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

(1)　役員　地方独立行政法人大阪市立工業研究所定款第８条に定める者をいう。

(2)　職員　地方独立行政法人大阪市立工業研究所職員就業規則第２条及び第３条第２項各号に定める者をいう。

(3)　職員等　職員及び、法人に派遣されている者をいう。

(4)　対象者　役員、職員等及び、法人が保有する情報資産を取り扱うすべての者とする。

(5)　情報資産　情報システム及び通信ネットワークで取り扱うデータやその運用管理に係るファイル（データを記録している電磁的記録をいう。以下同じ。）及びドキュメント（情報システムに関する文書をいう。）、並びに情報システム及び通信ネットワークを構成する機器をいう。

(6)　情報セキュリティ　情報に対し、次の性質を維持することをいう。

ア　機密性　情報資産へのアクセスを認められた者だけが、その情報資産にアクセスできる状態を確保すること。

イ　完全性　情報資産が破壊、改ざん又は消去されていない状態を確保すること。

ウ　可用性　情報資産へのアクセスを認められた者が、必要時に中断することなく、情報資産及び関連資産にアクセスできる状態を確保すること。

(7)　情報セキュリティ対策　情報セキュリティを確保するために実施する対策をいう。

(8)　システム運用対策　情報セキュリティ対策の中で、特にコンピュータ等を利用した情報ネットワークシステムの運用についての対策をいう。

(9)　情報セキュリティの侵害　情報の流失、漏洩、改ざん、破壊、障害等により情報資産が侵害されることをいう。

（情報資産の対象範囲）

第３条　この規程が対象とする情報資産は、対象者が業務上作成し、収集し、又は取得した、次の各号に定めるものとする。

(1)　法人が所有する産業技術に関する情報

(2)　法人が実施する支援業務に関する情報

(3)　法人が所有する知的財産及びそれに関する情報

(4)　法人の施設、設備機器及び情報システムに関する契約文書、取扱説明書、使用許諾証明書

(5)　その他法人の運営に必要な文書などの情報

第２章　組織体制及び責務

（最高情報統括責任者）

第４条　法人に最高情報総括責任者を置き、理事長を充てる。

２　最高情報統括責任者は、基本方針を制定する。
３　最高情報統括責任者は、情報セキュリティ対策状況の監査を行う。
４　最高情報統括責任者は、第８条に定めるシステム運用管理者を任命する。

（情報セキュリティ責任者）

第５条　法人に情報セキュリティ責任者を置き、経営企画担当理事を充てる。
２　情報セキュリティ責任者は、法人における情報セキュリティ対策に関する最高決定権限及び責任を有する。

（情報セキュリティ責任者の責務）

第６条　情報セキュリティ責任者は、第７条に定める情報管理責任者に対して、情報セキュリティ対策の統一的な実施のための指導、助言又は調整を行う。
２　情報セキュリティ責任者は、情報資産を維持、管理するため、各種記録等の保管を行う
３　情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、報告体制の整備を行う。
４　情報セキュリティ責任者は、基本方針及び本規程（以下「基本方針等」という。）の遵守のため、対象者に対する教育、訓練、助言及び指示を行う。

（情報管理責任者）

第７条　法人の各部にそれぞれ情報管理責任者を置き、各部長を充てる。
２　情報管理責任者は、各部に所属する対象者に対して、情報セキュリティ対策が適切かつ確実に実施されるように指導、助言又は調整を行う。
３　情報管理責任者は、各部に関する情報資産について管理責任を有し、当該情報資産における事故・欠陥等に対して、情報セキュリティ対策が適切かつ確実に実施されるように必要な措置を講じる。
４　情報管理責任者は、業務の遂行に緊急を要する等の場合、自己の判断にて必要かつ十分な情報セキュリティ対策を実施する決定権限と責任を有する。

（システム運用管理者）

第８条　法人の各情報システムにそれぞれシステム運用管理者を置く。
２　システム運用管理者は、当該情報システムのハードウェア及びソフトウェアが正常に稼動するように安全性に配慮し、適切なシステム運用対策を行う。
３　システム運用管理者は業務の遂行に緊急を要する等の場合、自己の判断にて必要かつ十分な情報セキュリティ対策を実施する決定権限と責任を有する。

（事務局）

第９条　情報セキュリティ責任者を補佐するため、事務局を置く。
２　事務局は、総務部が担当する。

第３章　情報資産の分類と管理

（情報資産の分類）

第１０条　情報セキュリティ責任者は、法人の情報資産について、機密性、完全性及び可用性を踏まえ、別表に定める重要性分類に従って分類し、アクセス制限を行う等、適切に管理する。

（情報資産の管理）

第１１条　情報管理責任者は、各部の情報資産を別表に定める重要性分類に基づき管理する。
２　情報資産が複製又は伝送された場合には、複製又は伝送された情報資産も別表に定める重要性分類に基づき管理する。
３　情報資産を取り扱う者は、情報資産の分類に応じて適切に取り扱うものとする。
４　情報資産を取得した者あるいは作成した者が取得等した情報資産についてその分類が不明な場合は、情報管理責任者に判断を仰がなければならない。

５　対象者は、業務上必要のない情報を取り扱ってはならない。
６　情報資産の分類が異なる複数の情報を取り扱う場合は、別表に定める重要性分類における最高度の分類に従って取り扱うものとする。

（情報セキュリティ対策）

第１２条　情報セキュリティ責任者は、物理的な情報セキュリティ対策として、次の各号に定める項目を管理する。
(1)　管理区域の管理
(2)　情報資産を取り扱うために必要な設備の管理

第１３条　情報セキュリティ責任者は、技術的な情報セキュリティ対策として、次の各号に定める項目を管理する。
(1)　ハードウェアの導入・調達・保守・管理
(2)　ネットワークの維持・管理
(3)　情報システム及び情報サービスの導入・調達・開発・管理
(4)　セキュリティ侵害対策・違反防護策等の導入・維持・管理

第１４条　情報セキュリティ責任者は、人的な情報セキュリティ対策として、次の各号に定める項目を管理する。
(1)　対象者の遵守事項
(2)　研修・訓練
(3)　事故・欠陥等の報告
(4)　ユーザアカウント・パスワード等の管理

（研修・訓練）

第１５条　情報セキュリティ責任者は、対象者に対して情報セキュリティに関する研修や訓練を適宜実施する。

（研修・訓練への参加）

第１６条　対象者は、定められた研修・訓練に参加しなければならない。

（ユーザアカウントの取り扱い）

第１７条　対象者は、自己のユーザアカウントを自己以外の者に使用されないように、適切に管理する。

（パスワードの取り扱い）

第１８条　対象者は、自己の管理するパスワードに関し、次の各号に定める事項を遵守する。
(1)　自己のパスワードを自己以外の者に使用されないように、適切に管理する。
(2)　パスワードは３か月ごとに変更しなければならない。

（事故・欠陥等の対応）

第１９条　対象者は、情報セキュリティに関する事故・欠陥等を発見した場合、速やかに所属する部の情報管理責任者に報告する。
２　情報管理責任者は、前項で報告された事故・欠陥等に対して、情報セキュリティ対策が適切かつ確実に実施されるように必要な措置を講じる。ただし、事故・欠陥等の内容に応じて、該当する情報システムのシステム運用管理者と必要かつ十分な協議、連携を行うものとする。
３　情報管理責任者は、第１項で報告された事故・欠陥等のうち、情報セキュリティの侵害が発生する又は侵害のおそれがある等、重大であると判断するもの（以下「重大事故等」という。）については、措置内容等と併せて、速やかに情報セキュリティ責任者に報告する。
４　情報セキュリティ責任者は、前項で報告された重大事故等について、最高情報統括責任者に報告する。
５　情報セキュリティ責任者は、重大事故等に関して外部から陳情や報告を受ける必要があると判断する場合は、そのための窓口を設置し、当該窓口への報告手段を公表する。

（重大事故等の記録）

第２０条　情報セキュリティ責任者は、前条第３項で報告を受けた重大事故等に関する記録を適切に保管する。

第４章　基本方針等の遵守

（対象者の遵守事項）

第２１条　対象者は、基本方針等を遵守しなければならない。

２　対象者は、異動、退職等により法人の業務を離れる場合には、利用していた情報資産を法人に返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

（外部委託事業者への対応）

第２２条　情報セキュリティ責任者は、情報資産を取り扱う業務を外部委託事業者に委託する場合、外部委託事業者から再委託を受ける事業者も含めて、当該事業者に基本方針等を理解させ遵守させなければならない。

（基本方針等の遵守状況の点検）

第２３条　情報管理責任者は、各部における基本方針等の遵守状況について自己点検を各年度１回行い、自己点検結果を情報セキュリティ責任者に報告する。

２　情報セキュリティ責任者は、前項で報告された自己点検結果をとりまとめ、問題と認める場合は適切かつ速やかに措置を講じるとともに､最高情報統括責任者にその内容を報告する。

（情報システムの運用管理状況の点検）

第２４条　システム運用管理者は、当該情報システムの運用管理状況を随時点検し、問題と認める場合は速やかにその問題状況を最高情報統括責任者に報告する。

２　最高情報統括責任者は、前項で報告された情報システムの運用管理上の問題を情報セキュリティ責任者に通知する。

３　情報セキュリティ責任者は､前項で通知された情報システムの運用管理上の問題に対して、対策が必要であると判断する場合は適切かつ速やかに措置を講じる。

４　情報セキュリティ責任者は、前項で措置を講じた結果について、最高情報統括責任者に報告する。

（情報資産の取扱状況調査）

第２５条　情報セキュリティ責任者は、基本方針等の遵守状況の調査のため、対象者が使用するパーソナルコンピュータ等の端末、記録媒体のアクセス記録、電子メールの送受信記録等の利用状況を調査することができる。

２　情報セキュリティ責任者は、前項の調査を指名した者に行わせることができる。

３　情報セキュリティ責任者は、第１項の調査結果を最高情報統括責任者に報告する。また、調査を行ったことを調査の対象となった対象者に告げなければならない。

（基本方針等に対する違反の対応）

第２６条　対象者は、基本方針等に対する違反行為を発見した場合、直ちにその内容を情報セキュリティ責任者に報告する。

２　情報セキュリティ責任者は、前項における報告又は前条に定める情報資産の取扱状況調査において、対象者の基本方針等に対する違反行為を確認した場合、当該違反者が所属する部の情報管理責任者に通知し、改善措置を求める。

３　情報管理責任者は、前項で求められた改善措置に対して、当該違反者に適切な指導、助言等を行い、改善を図る。

４　前項の改善措置が達せられない場合、情報セキュリティ責任者は、当該違反者の情報資産の取り扱いを停止するなど、速やかに適切な措置を行う。

（自己点検、違反行為等の記録の保管）

第２７条　情報セキュリティ責任者は、第２３条第１項に定める情報管理責任者の自己点検結

果、第２４条第３項に定める情報システムの運用管理上の問題点及び措置結果、並びに第２６条第２項に定める基本方針等に対する違反行為の内容及び対策等の記録を適切に保管する。

（懲戒処分）

第２８条　基本方針等に違反した職員及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方独立行政法人大阪市立工業研究所職員懲戒規程に基づき設置される職員懲戒審査委員会において審議され、地方独立行政法人大阪市立工業研究所就業規則第５４条に定める懲戒処分を受ける。

第５章　情報セキュリティの侵害への対応

（緊急時対応計画の策定）

第２９条　情報セキュリティ責任者は、情報セキュリティの侵害が発生した場合又は発生するおそれがある場合に、報告、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するため、緊急時対応計画を策定する。

（緊急時対応計画の内容）

第３０条　緊急時対応計画には、次の各号に定める事項を含める。

(1)　関係者の連絡先

(2)　発生した事案に係る報告すべき事項

(3)　発生が想定される事案への対応措置

（緊急時対応計画の見直し）

第３１条　情報セキュリティ責任者は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画を見直す。

（例外措置の許可）

第３２条　情報管理責任者は、業務の適正な遂行を継続するため、例外的に情報セキュリティの遵守事項とは異なる方法を採用すること又は遵守事項を実施しないこと（以下「例外措置」という。）について合理的な理由がある場合は、情報セキュリティ責任者に例外措置の許可を求めることができる。

２　システム運用管理者は、当該情報システムの運用にかかる業務の適正な遂行を維持するため、例外措置について合理的な理由がある場合は、最高情報統括責任者に例外措置の許可を求めることができる。最高情報統括責任者は、許可を求められた例外措置について情報セキュリティ責任者に通知する。

３　情報セキュリティ責任者は、第１項で許可を求められた例外措置又は前項で通知された例外措置について、その妥当性を判断し、当該の例外措置を許可することができる。

（緊急時の例外措置）

第３３条　情報管理責任者及びシステム運用管理者は、業務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは自己の判断において例外措置を実施することができる。

２　情報管理責任者は、前条第１項に定める許可を得ずに実施した緊急時の例外措置について、事後速やかに情報セキュリティ責任者に当該例外措置を報告する。

３　システム運用管理者は、前条第２項に定める許可を得ずに実施した緊急時の例外措置について、事後速やかに最高情報統括責任者に当該例外措置を報告する。最高情報統括責任者は、当該の緊急時の例外措置を情報セキュリティ責任者に報告する。

（例外措置の対応）

第３４条　情報セキュリティ責任者は、第３２条及び前条に基づいて実施された例外措置について、情報セキュリティ対策が適切かつ確実に実施されるように必要な対応を講じる。

２　情報セキュリティ責任者は、前条の例外措置及びその対応について、最高情報統括責任者に報告する。

（例外措置の記録）
第３５条　情報セキュリティ責任者は、第３２条、第３３条及び前条における例外措置にかかる記録を適切に保管する。

第６章　外部委託

（外部委託事業者の選定基準）
第３６条　法人の情報資産を取り扱う業務を外部委託する場合、外部委託事業者の選定基準として、情報セキュリティ責任者は、委託内容に応じた情報セキュリティ対策が確保されることを確認する。
２　法人は、情報セキュリティマネジメントシステムの国際規格の認証取得状況等を参考にして、外部委託事業者を選定しなければならない。
（契約項目）
第３７条　法人は、情報システムの運用等を外部委託する場合、必要に応じて外部委託事業者との間で次の各号に定める情報セキュリティ要件を明記した契約を締結する。
(1)　基本方針等に関する法人規程類の遵守
(2)　委託先の責任者、委託内容、作業者、作業場所の特定
(3)　法人に提供されるサービスレベルの保証
(4)　従業員に対する教育の実施
(5)　法人から提供された情報の目的外利用及び委託者以外の者への提供の禁止
(6)　業務実施上知り得た情報の守秘義務
(7)　再委託に関する制限事項の遵守
(8)　委託業務終了時の情報資産の返還、廃棄等
(9)　委託業務の定期報告及び緊急時報告義務
（確認・措置等）
第３８条　情報セキュリティ責任者は、外部委託事業者が必要な情報セキュリティ対策を確保していることを適宜確認し、必要に応じて情報セキュリティ対策が適切かつ確実に実施されるように前条の契約に基づき措置を講じる。

第７章　法令遵守

（法令遵守）
第３９条　対象者は、職務の遂行において使用する情報資産を保護するために、次の各号に定める法令等のほか関係法令等を遵守し、これに従わなければならない。
(1)　地方独立行政法人法（平成１５年７月１６日法律１０８号）
(2)　著作権法（昭和４５年５月６日法律４８号）
(3)　不正アクセス行為の禁止等に関する法律（平成１１年８月１３日法律１２８号）
(4)　個人情報の保護に関する法律（平成１５年５月３０日法律５７号）
(5)　大阪市個人情報保護条例（平成７年３月１６日条例第１１号）

第８章　監査

（監査の実施）
第４０条　最高情報統括責任者は、情報セキュリティ対策状況についての監査を必要に応じて実施できる。
２　監査を受ける対象者は、監査の実施に協力しなければならない。
３　監査の実施方法その他必要な事項は、最高情報統括責任者が定める。
（監査結果への対応）
第４１条　最高情報統括責任者は、監査結果を踏まえて必要があると認めるときは講じるべき改善措置の内容を定め、情報セキュリティ責任者に対して当該改善措置の実施を求める。
２　情報セキュリティ責任者は、前項で求められた改善措置を適切かつ確実に実施しなければ

ならない。

第９章　その他

（基本方針等の見直し）

第４２条　最高情報統括責任者は、監査の結果並びに基本方針の定めに応じて、必要があると認める場合、基本方針等を見直す。

（その他）

第４３条　この規程に定めるもののほか、必要な事項については別途理事長が定める。

附　則

この規程は、平成２７年３月〇〇日から施行する。

別表（第１０条、第１１条関係）

情報資産の重要性分類
Ⅰ　個人情報及び業務上必要とする最小限の者のみが扱う情報資産 Ⅱ　外部への公開を行うべきでない情報資産 ・法令等の定めにより守秘義務が課せられている情報資産 ・外部に知られることを適当としない法人等に関する情報資産 ・漏えいした場合、法人に対する信頼を著しく阻害するおそれのある情報資産 Ⅲ　法人業務運営上の重要な情報資産 ・滅失し、又はき損した場合、その復元が著しく困難であり、法人の円滑な運営を妨げるおそれのある情報資産 Ⅳ　上記以外の情報資産